F. # 2019R000644

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF THE PREMISES KNOWN AND DESCRIBED AS 109-33 46TH AVENUE, 3RD FLOOR, QUEENS, NEW YORK 11368, INCLUDING ANY AND ALL LOCKED AND CLOSED CONTAINERS, APPURTENANT STORAGE SPACES AND ELECTRONIC DEVICES FOUND THEREIN	**TO BE FILED UNDER SEAL** **AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT FOR PREMISES AND ELECTRONIC DEVICES FOUND THEREIN** Docket No. 21-692-M

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, ADAM RODRIGUEZ, being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations ("HSI") for over four years, duly appointed according to law and acting as such.

2. In my capacity as a Special Agent with HSI, I have conducted and participated in official investigations into fraud, money laundering and other financial crimes as well as numerous cases involving fraudulent documents. I also have conducted or participated in electronic and physical surveillance, the execution of search warrants, and debriefings of informants.

3. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises described in Attachment A (the "Subject Premises") for the items and information listed in Attachment B.

4. The facts in this affidavit come from my personal observations, my review of documents and other materials, my training and experience and information obtained from other agents and witnesses. This affidavit is intended to show only that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF PREMISES

5. The Subject Premises is the third story and appurtenant storage areas of a three-story brick apartment building with a white front door located at 109-33 46th Avenue in Corona, Queens, New York, and any and all locked and closed containers and electronic devices located therein. Three mailboxes and a security camera are affixed to the wall outside of the Subject Premises. A photograph of the outside of the Subject Premises is included in Attachment A and below. This application seeks permission to search the third-floor apartment and any storage units within the building that are appurtenant to the third-floor apartment, any and all locked and closed containers and electronic devices located therein for the items and information described in Attachment B.

PROBABLE CAUSE

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that the Subject Premises, including locked and closed containers and electronic devices located therein, contain evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1028(a) and (f) (fraud

related to identification documents) and Title 18, United States Code, Section 1028A (aggravated identity theft) (together, the "Subject Offenses").

I. The Conspiracy to Create and Sell False Identification Documents

7. Since 2018, HSI has been investigating a false identification document manufacturing and distribution ring in the Corona neighborhood of Queens, New York (the "Ring"). Law enforcement first learned about the Ring through a confidential source ("CS-1").[1] Based on my participation in this investigation, I have learned that the Ring creates and sells false Lawful Permanent Resident cards ("LPR Cards"), passports, Social Security cards, and driver's licenses.

II. The Controlled Purchases

8. Between November 2018 and May 2019, HSI agents conducted a series of controlled purchases of false documents through a confidential source ("CS-2").[2] In particular,

---

[1] CS-1 has been providing information to HSI for approximately eight years. CS-1 was arrested in 2013, convicted of selling false identification documents in violation of 18 U.S.C. § 1028 and served 12 months of supervised release. Although CS-1 currently has temporary lawful immigration status, CS-1 did not have legal immigration status in the United States during much of this investigation and was therefore subject to deportation as a result of a criminal conviction. CS-1 has provided extensive information to HSI in exchange for deferred immigration action. The information CS-1 has provided has been deemed credible and has been corroborated by independent evidence.

[2] CS-2 has been a confidential source for HSI for approximately eleven years. CS-2 was arrested in 2006 but was not convicted. CS-2 was also administratively charged in 2010 with being unlawfully within the United States. Since that time, CS-2 has been working with HSI in exchange for deferred immigration action, as well as financial compensation. The information CS-2 has provided has been deemed credible and has been corroborated by independent evidence.

at the direction of law enforcement, CS-2 approached a member of the Ring ("CS-3")[3] and asked to purchase false documents. Over the course of four transactions, CS-2 purchased five paper Social Security cards, five plastic LPR Cards, and one plastic driver's license. The interactions between CS-2 and CS-3 were video recorded.

9. In one interaction, for example, CS-2 approached CS-3. CS-2 asked CS-3 if CS-3 knew the people who sold false identification documents. CS-3 indicated that CS-3 could provide false identification documents and showed CS-2 examples of false identification documents. CS-3 told CS-2 the price for one Social Security card and one LPR Card, and took a photograph of CS-2 for the LPR Card. The next day, CS-2 paid CS-3 cash for the cards. CS-3 confirmed that more false identification documents could be provided.

10. The identification documents obtained by CS-2 from CS-3 were subsequently turned over to law enforcement, which confirmed that the documents were falsified. Specifically, the documents were submitted to the HSI forensic laboratory for testing, and the laboratory confirmed that the documents were not genuine. Moreover, law enforcement requested and received confirmation from the Social Security Administration, Office of the Inspector General, that the Social Security numbers on the Social Security cards did not match the names printed on the cards. Certain of the purchased cards included real personal identifiers, including Alien Registration Numbers and/or Social Security numbers, that belong to individuals other than those named on the cards.

---

[3] CS-3 pleaded guilty on April 13, 2021, to conspiracy to commit an offense against the United States, in violation of Title 18, United States Code, Section 371, for conspiring to create and sell false identification documents, contrary to Title 18, United States Code, Section 1028(a), in connection with the conduct set forth herein. See 21-CR-178 (DG). CS-3 is cooperating with the government in exchange for sentencing consideration.

III. Information Provided by CS-3

11. After the controlled purchases were complete, HSI agents approached CS-3, and CS-3 agreed to cooperate with law enforcement.

12. During a July 1, 2019 interview with HSI, CS-3 reported that in approximately 2016, CS-3 began to work with certain individuals, most or all of whom I believe to be members of the Ring, and to assist with distribution of the false identification documents in exchange for cash payments. In particular, CS-3 served as a customer liaison for the Ring, taking orders from customers and passing along those orders to other members of the Ring who would then create the false documents.

13. CS-3 informed law enforcement that there were many members of the Ring and that CS-3 knew some of their "street" names: in particular, individuals known as "CHELI," "RONI," "BRAULIO" and "MYSTERIO," among others.[4] CS-3 explained that the false identification documents created by the Ring were typically constructed from either paper or hard plastic. According to CS-3, several members of the Ring, including RONI, manufactured the paper documents, and CHELI made high-quality plastic documents on a machine. CS-3 believed the machine used by CHELI was located in CHELI's residence, which

[4] CHELI, RONI, BRAULIO and MYSTERIO were indicted on June 4, 2021, by a grand jury sitting in the Eastern District of New York, and charged with conspiracy to manufacture and distribute false identification documents, in violation of Title 18, United States Code, Sections 1028(a) and (f). Docket No. 21-cr-305 (WFK) (the indictment is annexed hereto as Exhibit A and incorporated herein by reference). Arrest warrants for each of the defendants are expected to be executed in conjunction with the applied-for search warrant.

CS-3 stated was an apartment in Queens from which Flushing Meadows Park can be seen. CS-3 stated that CHELI was the leader of the Ring.[5]

IV. Identification of CHELI and the Subject Premises

14. As explained further below, the evidence obtained in this investigation indicates that CHELI's true name is JOSE LUIS GASPAR and that he lives in the Subject Premises. Specifically, CS-1 informed law enforcement of CHELI's cellular telephone number, (the "Subject Phone"). Based on a review of law enforcement databases and public records, law enforcement was able to determine that the Subject Phone was associated with the Subject Premises. Based on this and other information, including surveillance, reports from cooperating sources and records obtained from the United States Postal Service, law enforcement was able to determine that CHELI's real name is JOSE GASPAR. The name JOSE GASPAR is also associated with the Subject Premises. On numerous occasions during surveillance of the Subject Premises, law enforcement observed and photographed a man who matched CS-1's and CS-3's descriptions of CHELI entering and leaving the Subject Premises. Both CS-1 and CS-3 viewed one of the photographs and confirmed that the individual depicted in the photograph was CHELI.

15. Surveillance further showed the individual using a key to access the mailbox associated with the third-floor apartment, as well as repeatedly looking out from behind a sliding glass door, which permits egress to a third-floor balcony. Investigators confirmed with a Postal Inspector that packages addressed to JOSE LUIS GASPAR were mailed to the third

---

[5] CS-1, who is familiar with several members of the Ring and with the false document scheme as a whole, likewise informed law enforcement that CHELI was in charge of the scheme.

floor of the Subject Premises. Additionally, it appears that Flushing Meadows Park would be visible from the third-floor window of the Subject Premises. Finally, CS-3 informed law enforcement that CHELI is RONI's uncle; JOSE LUIS GASPAR and RONI GASPAR share the same last name. I therefore believe CHELI's true name is JOSE LUIS GASPAR and that he resides at the Subject Premises.

16. When CS-3 first began working with the Ring in 2016, members of the Ring provided CS-3 a "burner" cellular telephone to use in carrying out the scheme.[6] Customers typically approached CS-3 directly or sent text messages to the cellular telephone with orders for false identification documents. CS-3 then either spoke with or used the cellular telephone to text the information to a member of the Ring so that the false identification documents could be created. Once the documents were ready, a runner from the Ring, including but not limited to BRAULIO and MYSTERIO, would bring them to CS-3 for delivery; CS-3 gave the false documents to customers and received payment in cash. A member of the Ring – often the same runner who dropped off the documents – later picked up the cash and paid CS-3 a portion of it. CS-3 admitted to having assisted in generating at least one hundred false documents in a six-month period alone.

17. Through surveillance of the Subject Premises, law enforcement also observed another individual, Individual-1, who CS-3 confirmed was a runner for the Ring, approach the Subject Premises, stand outside the front door and manipulate his cellular telephone, during which time it appeared that Individual-1 was sending text messages, then enter

[6] A "burner" phone is a cellular telephone, often purchased in conjunction with a pre-paid service plan, that is not registered under the user's name or is otherwise anonymized for the purpose of concealing the user's identity.

the Subject Premises. Individual-1 exited the Subject Premises less than one minute after entering. Over the course of approximately one year, law enforcement observed at least a dozen instances of Individual-1 approaching, entering, and leaving the Subject Premises in a similar manner. On at least one such occasion law enforcement observed Individual-1 approach the Subject Premises after having been seen in the vicinity of CS-3 approximately three hours before. On another occasion, law enforcement observed Individual-1 approach CS-3 with a white envelope in hand approximately fifteen minutes after leaving the Subject Premises. Based on my experience and training as a law enforcement officer and my knowledge of this investigation, I believe that Individual-1 entered the Subject Premises to pick up false identification documents, and he then brought those documents to CS-3 to fulfill the orders.

V. Recent Activities of the Ring

18. As recently as approximately mid-April 2021, CS-3 confirmed that false identification documents continued to be sold by the Ring. Members of the Ring have continued to ask CS-3 to take photographs of individuals for false identification documents.

19. On numerous occasions and most recently on or about April 28, 2021, during surveillance of the Subject Premises, law enforcement observed an individual, Individual-2, approach the Subject Premises and stand outside the front door. Individual-2 manipulated his cellular telephone, during which time it appeared that Individual-2 was sending text messages, and entered the Subject Premises. Less than one minute later, Individual-2 exited the Subject Premises.

20. Law enforcement agents showed several surveillance photographs of Individual-2 to CS-1. CS-1 is familiar with Individual-2 and knows him to be a member of the Ring. CS-1 informed law enforcement that Individual-2's role is to pick up documents from the

homes of CHELI and BRAULIO and hand them out to customers on the street. CS-1 further noted that CS-1 had seen Individual-2 on the street distributing documents as recently as approximately one week ago, although CS-1 was not aware of whether Individual-2 had obtained those particular documents from CHELI or BRAULIO.

21. Based on the similarities in the conduct of Individual-1 and Individual-2, the information provided by CS-1 my experience and training as a law enforcement officer and my knowledge of this investigation, I believe Individual-2 is also a runner for the Ring and that he entered the Subject Premises to conduct transactions related to false identification documents.

22. On or about May 11, 2021, law enforcement observed a transaction between MYSTERIO and BRAULIO, in which the two met and exchanged a white object.

VI. Additional Probable Cause Related to the Subject Premises

23. Based on the foregoing, as well as my experience and training as a law enforcement officer, I believe that evidence of the Subject Offenses will be found within the Subject Premises, as set forth in this paragraph and in further detail below. In particular, I believe that the Subject Premises will contain completed and partially-completed false identification documents as well as paraphernalia related to the creation of false identification documents such as plastic laminating materials, paper cutters, paper and ink.

24. In my experience, I have found that people who sell false identification documents and other unlawful items frequently maintain hard copy or electronic books, records, ledgers and other such information pertaining to the operation of the unlawful business, as well as proceeds of the business in the form of cash. I have also found that unlawful businesses that generate significant quantities of cash, such as the scheme described herein, commonly take measures to launder some or all of the proceeds. Such measures can result in the creation of

physical records such as bank deposit receipts, money orders and other evidence. I therefore believe that records and information pertaining to the sale of false identification documents and the disposition of the proceeds therefrom are likely to be found within the Subject Premises, as well as the proceeds themselves.

25. Further, because the information obtained during this investigation indicates that CHELI is the leader of the Ring, I believe he may possess within the Subject Premises documents, records and information pertaining to the operations of the Ring.

26. The materials referenced above are easily portable. Moreover, items such as paper cutters and laminating machines can be large and take up a significant amount of space. Accordingly, to the extent there is a storage unit appurtenant to the apartment within the building, this application seeks approval to search such storage units as well as the third-floor apartment itself.[7]

VII. Additional Probable Cause Related to Electronic Devices

27. I also believe that the Subject Premises will contain electronic devices used to create and communicate about false identification documents. In particular, as noted above, CS-3 reported to law enforcement that CHELI used a "machine" to manufacture the false identification documents, and that CS-3 used a cellular telephone to transmit photographs and information to members of the Ring for the purpose of creating false identification documents. In light of the electronic transmission of the photographs and information, and in light of the

[7] Because the building in which the Subject Premises are located is small, consisting of only two or three units, law enforcement has not been able to conduct surveillance within the building. However, publicly-available records indicate that the building contains an unfinished basement which may provide storage for the building's tenants. This application seeks to search any storage space within the building that is assigned to the Subject Premises.

high quality of the false identification documents created by the machine, I believe that the machine described by CS-3 can either be connected to the Internet or receive data through some sort of file transfer interface, including but not limited to a connection to a computer, cellular telephone or server network. This application therefore seeks approval to seize electronics, including but not limited to printers and computers (including but not limited to cellular telephones), that may be located within the Subject Premises.[8]

28. Further, it is my belief, based on the foregoing and my training and experience, that CHELI used cellular telephones, including but not limited to the Subject Phone, to communicate regarding the Subject Offenses. Phone records obtained during the investigation reflect dozens of calls in a three-month period between CHELI's and RONI's cellular telephones. Moreover, in most, if not all, instances in which Individual-1 and Individual 2 entered the Subject Premises, they first stood outside the door of the building and manipulated cellular telephones, evidently sending text messages. The regularity with which Individual-1 and Individual-2 apparently sent text messages prior to entering the Subject Premises is suggestive that Individual-1 and Individual-2 were using the cellular telephones to text CHELI or other co-conspirators before entering. Finally, as was also discussed above, members of the Ring provided CS-3 with a cellular phone so that CS-3 could text information

---

[8] Based on the investigation, it appears that CHELI lives in the Subject Premises with his wife and possibly his daughter. This application does not seek to search any electronic devices belonging solely to and used solely by CHELI's wife and daughter, to the extent such electronic devices also contain no evidence of the Subject Offense. However, it may be difficult to identify such devices during the course of the search. In order to avoid unreasonably prolonging the search, law enforcement agents may seize devices as to which the use or ownership is not immediately clear, and then return any seized devices promptly if and when it is determined that CHELI does not own or use the devices and that such devices contain no evidence of the Subject Offense.

and photographs to members of the Ring. It is reasonable to believe that the members of the Ring then passed the information from CS-3 along to CHELI by text message so that CHELI could manufacture the documents. I therefore believe that CHELI's cellular telephone is likely to contain evidence, fruits and instrumentalities of the Subject Offenses.

29. Additionally, based on my training and experience, I know that people who commit crimes such as the Subject Offenses sometimes use "burner" cellular telephones to communicate with co-conspirators. As discussed herein, I know that at least some members of the Ring, including CS-3, used "burner" phones provided by the Ring in order to communicate regarding customers' orders of false identification documents. Further, according to subpoena returns, at least one cellular telephone number (besides the Subject Phone) that CHELI used to contact other members of the Ring was tied to an anonymized pre-paid service plan, suggesting that that particular cellular telephone is a "burner" cellular telephone. I therefore believe that a "burner" cellular telephone may be found within the Subject Premises. To the extent law enforcement encounters additional cellular telephones within the Subject Premises that do not belong to CHELI's wife or another resident, this application seeks authorization to search the additional cellular telephone(s) and seize the materials set forth in Attachment B.

30. Finally, there appears to be a security camera affixed to the wall outside of the Subject Premises. To the extent that footage from the security camera is stored in the Subject Premises, such footage would constitute evidence of the Subject Offenses insofar as it would reflect the visits paid by Individual-1, Individual-2 and others to the Subject Premises for the purpose of picking up completed false identification documents.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

31. As described above, there is probable cause to believe that a machine used to create false identification documents will be found in the Subject Premises. As described above and in Attachment B, this application seeks permission to search for and seize the machine as well as data transmitted to or from the machine related to the creation of false identification documents that might be found in the Subject Premises, in whatever form they are found. One form in which the data might be found is on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

32. *Probable cause.* I submit that if a computer[9] or storage medium[10] is found on the Subject Premises that is physically connected by wire to, or capable of wireless or hard-wired connection with, a machine present in the Subject Premises that could be used to make false identification documents, there is probable cause to believe that data related to false identification documents are stored on that computer or storage medium, for at least the following reasons:

a. Based on my experience and training as a law enforcement officer, my conversations with other law enforcement officers and the evidence in this case, including

---

[9] A computer includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptops, mobile phones, tablets, servers and network hardware, such as wireless routers.

[10] A "storage medium" for purpose of the requested warrant is any physical object upon which computer data can be recorded. Examples include external hard drives, CDs and DVDs, and flash drives.

but not limited to the statements of CS-1, CS-2 and CS-3 and surveillance conducted by law enforcement officers, there is probable cause to believe that the device used to make false plastic identification documents is located at the Subject Premises. In my experience, devices of this sort may involve multiple components, including lamination machines, cutters, and printers. These components often interface with a computer, and may be connected to a computer either by cable or by Wireless Fidelity ("wifi"). There is therefore probable cause to believe that a computer involved in the creation of false identification documents is located in the Subject Premises.

b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

c. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

d. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer

has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

e. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

33. *Forensic evidence.* As further described in Attachments A and B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the Subject Premises because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information

about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a

particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

34. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

35. *Nature of the examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

36. Because people other than CHELI appear to live in the Subject Premises, it is possible that the Subject Premises will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that there is probable cause that the things described in this warrant could be

found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.[11]

DOCUMENTS AND RECORDS

37. As described above, there is probable cause to believe that JOSE LUIS GASPAR lives at the Subject Premises, that he is the leader of the false identification document Ring, and that he manufactures false identification documents at the Subject Premises. I therefore believe that the Subject Premises will contain documents and records related to the Ring, including the documents and records described in Attachment B. Specifically, from the foregoing, I have learned, among other things, the following:

a. Based on my experience and training, as well as conversations with other law enforcement officers, I am aware that, during the execution of search warrants in false identification document investigations, documents and records of the type described in Attachment B have been found during the execution of search warrants at the locations where false identification documents are manufactured, even where the location is not the ultimate point of sale. Such documents and records include, but are not limited to: false identification documents and/or partially completed false identification documents; fraudulently obtained personal identifying information used in manufacturing such identification documents; false identification document making equipment; electronic devices such as tablets and computers that connect to false identification document making equipment; records of correspondence or

[11] As set forth above, this application does not seek to seize any electronic devices that belong solely to and are used solely by CHELI's wife or other residents of the Subject Premises, to the extent such electronic devices also do not contain evidence of the Subject Offense.

communications conducted in the course of producing false identification documents; telephone records; ledgers, logs, financial records or other documents reflecting the sale of false identification documents; information regarding others involved in the false identification document trade; and fruits of participating in the production of false identification documents.

b. Individuals manufacturing such false identification documents often maintain close at hand the addresses and telephone numbers of their criminal associates, photographs of their associates, records of communications or correspondence with their associates, and information pertaining to their sources of supply and customers, in address books, electronic organizers and on other media, physical or electronic. Telephone bills and records of calls to telephones are also maintained for lengthy periods of time in such homes. Such records constitute important corroborative evidence in conspiracy cases because the defendants call one another regularly, especially just before and after an incident involving an act committed in furtherance of the conspiracy. Further, such records provide access to those who are purchasing and potentially redistributing false identification documents.

38. Based on my experience and training, as well as conversations with other law enforcement officers, I am aware that considerable amounts of cash are sometimes found during the execution of search warrants in false identification document investigations. Based on my experience and training, I am aware that the sale of false identification documents is a cash business, and when large amounts of cash are found at the residence of a co-conspirator in a false identification document conspiracy, there is probable cause to believe that such cash represents fruits of the scheme. Based on my participation in this investigation, I know that the co-conspirators provided false identification documents in exchange for cash. I also know that the runners that transmitted false identification documents from the Subject Premises to

customers would also pick up cash and transport it elsewhere. When a search warrant is executed at the Subject Premises, if significant amounts of cash are found, there is probable cause to believe that that cash represents the proceeds of the Ring's creation and sale of false identification documents.

39. In addition, based on my experience and training, I know that individuals who participate in cash businesses such as the scheme described herein often transfer the cash using wire services such as Western Union, or convert the cash into forms that can be more readily concealed, such as money orders. I also know that the materials used to fabricate false identification are generally purchased from commercial sources, including sources located overseas. Such materials are typically paid for by credit cards or other fund transfer vehicles. Accordingly, there is probable cause to believe that financial records and financial instruments within the Subject Premises, including but not limited to cash-equivalent instruments, constitute evidence, fruits and instrumentalities of the Subject Offenses.

CONCLUSION

WHEREFORE, I respectfully request that a search warrant issue, allowing HSI agents, with proper assistance from other law enforcement officers and agents, to search the Subject Premises and appurtenant storage spaces particularly described in Attachment A, including the Subject Phone and any electronics and locked and closed containers and items contained therein, and to seize the property described in Attachment B, all of which constitutes evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 1028(a), 1028(f) and 1028A.

IT IS FURTHER requested that this application be placed under seal until further order of this Court, to protect the integrity of the investigation described above, to ensure that no target of this investigation flees and to ensure the safety of the agents and others.

ADAM J RODRIGUEZ

Digitally signed by ADAM J RODRIGUEZ
Date: 2021.06.14 14:30:56 -04'00'

ADAM RODRIGUEZ
Special Agent
Homeland Security Investigations

Sworn to before me by telephone on
June 14, 2021

Marcia M. Henry

THE HONORABLE MARCIA M. HENRY
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

Property To Be Searched

The Subject Premises is the third story and appurtenant storage areas of a three-story brick apartment building with a white front door located at 109-33 46th Avenue in Corona, Queens, New York, and any and all locked and closed containers and electronic devices located therein. Outside the front door, three mailboxes and a security camera are affixed to the wall. A photograph of the outside of the Subject Premises is below. This application seeks permission to search the third-floor apartment as well as any storage units within the building that are appurtenant to the third-floor apartment.

ATTACHMENT B

DESCRIPTION OF THE ITEMS TO BE SEIZED

Items to be searched for, located and seized from the premises described in Attachment A, are those constituting evidence, fruits and instrumentalities of violations of Title 18, United States Code, Sections 1028(a) and (f) (fraud related to identification documents) and Title 18, United States Code, Section 1028A (aggravated identity theft) (the "Subject Offenses"), including, but not limited to, the following:

1. False identification documents, or any partially completed false identification documents, or personal identifying information used in the manufacturing of such identification documents.

2. Equipment used in the creation of false identification documents.

3. Financial records or documents, including: bank account records, credit card records, virtual wallet information, wire transfers, money transfer records, and money order records, reflecting transactions made in furtherance or with the fruits of the purchase and sale of false identification documents, as well as such records and documents pertaining to the purchase or sale of items or equipment used to produce such false identification documents.

4. All documents and communications created, exchanged in furtherance of or reflecting any and all steps taken in order to carry out the Subject Offenses.

5. Documents constituting or reflecting correspondence or communications pertaining to or in furtherance of the Subject Offenses, including but not limited to communications regarding the production, advertisement and sale of such false identification documents.

6. Documents and communications relating to any co-conspirators or any individuals involved in or with knowledge of the Subject Offenses, including but not limited to the organization and operation of the conspiracy to create and sell false documents.

7. All safes, including any contents of the safes that relate to the Subject Offenses, including financials, business contracts, proceeds, and any other items described in other paragraphs of this affidavit.

8. Telephone billing and toll records.

9. Fruits of the Subject Offenses, including funds or monetary instruments being used in or derived from the commission of such activities.

10. Documents and communications relating to or reflecting the disposition of the proceeds of the Subject Offenses.

11. Security camera footage stored within the Subject Premises from the camera located outside of the Subject Premises.

12. Electronic devices constituting, or capable of connecting (whether physically or wirelessly) to, false identification document making equipment, including without limitation computers, tablets, printers, scanners, keyboards, video display monitors, optical readers, and related communications devices such as modems, including but not limited to the devices specified in Paragraph 14 below.

13. Documents and communications tending to provide context to, or demonstrate custody and control of, any items or information described herein.

14. Computers[12] or storage media[13] that contain records or information (each a "Computer" and, together, the "Computers") used as a means to commit the Subject Offenses, including but not limited to any cellular telephone owned and/or primarily used by JOSE LUIS GASPAR. All information obtained from such Computers will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing information that constitutes fruits, evidence and instrumentalities of the Subject Offenses, including, as to each Computer:

a. evidence of who used, owned or controlled the Computer at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs and correspondence, including records that help reveal the whereabouts of such person(s) at various times;

b. evidence indicating the Computer owner's/user's state of mind as it relates to the Subject Offenses;

c. the identity of the person(s) who communicated with the Computer about matters relating to the Subject Offenses, including records that help reveal their whereabouts;

d. any and all bank records, account information and other financial records;

e. evidence indicating how and when the Computer was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the Computer's owner(s);

---

[12] A "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptops, mobile phones, tablets, servers and network hardware, such as wireless routers.

[13] A "storage medium" for purpose of the requested warrant is any physical object upon which computer data can be recorded. Examples include external hard drives, CDs, DVDs and flash drives.

f. evidence of software that would allow others to control the computers, such as viruses, Trojan horses and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

g. evidence of the lack of such malicious software;

h. evidence of the attachment to the Computers of other storage devices or similar containers for electronic evidence;

i. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Computer;

j. evidence of the times the Computer was used;

k. passwords, encryption keys and other access devices that may be necessary to access the Computer;

l. documentation and manuals that may be necessary to access the Computer or to conduct a forensic examination of the Computer;

m. contextual information necessary to understand the evidence described in this Attachment; and

n. all records, data and information in the Computer, including names and telephone numbers, as well as the contents of all call logs, contact lists, text messages (including but not limited to SMS, MMS, iMessage and WhatsApp messages), Google Hangouts or other chats, emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, location data, Internet activity (including browser history, web page logs, and search terms entered by the user), geo-location data, application data, and other electronic media, and other electronic data, constituting or reflecting any of the items set forth above, including but not limited to all records constituting or reflecting the documents and communications described in this Attachment B.

As used above, the terms “documents,” “data,” “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

If the government determines that possession of the physical Computers is no longer necessary to retrieve and preserve the data on the Computers, and that the Computers are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), the government will return the Computers upon request.